NASA Procedural Requirements

NPR 8000.4
Effective Date: April 25, 2002
Expiration Date: April 25, 2007

COMPLIANCE IS MANDATORY

Risk Management Procedural Requirements w/Change 1 (4/13/04)

Responsible Office: Office of Safety and Mission Assurance

TABLE OF CONTENTS

APPENDICES

Change History

NPR 8000.4, Risk Management Procedures and Guidelines, w/Change 1, 4/13/04

Change #	Date	Description/Comments
1	4/13/04	Deletions of paragraph, references, etc, per Jennings memo dated 12/5/03 and administrative changes made throughout to change NPG to NPR.

Preface

P.1 PURPOSE

Risk Management (RM) (see Appendix A, Glossary) is an organized, systematic decisionmaking process that efficiently identifies, analyzes, plans (for the handling of risks), tracks, controls, communicates, and documents risk to increase the likelihood of achieving program/project (see Appendix A, Glossary) goals. RM is therefore essential to sound program/project management and vital to safety and mission success. This NASA Procedural Requirement (NPR) provides the requirements and information for applying RM to programs and projects as required by NPR 7120.5, "NASA Program and Project Management Processes and Requirements," and as required by NPD 8700.1, "NASA Policy for Safety and Mission Success."

P.2 APPLICABILITY AND SCOPE

P.2.1 This NPR applies to NASA Headquarters and NASA Centers, including Component Facilities; and to the Jet Propulsion Laboratory (JPL) and other contractors to the extent specified in their respective contracts.

P.2.2 This document provides the basic processes and requirements for the planning and implementation of the RM process through the life cycle (see Appendix A, Glossary) of all programs and projects. It shall be used specifically for programs/projects that provide aerospace products or capabilities - i.e., flight and ground systems, technologies, and operations for space and aeronautics (Requirement 26001). It is not required for other projects (such as research conducted under the Generate Knowledge Crosscutting Process or training and education conducted under the Manage Strategically Crosscutting Process); however, the RM concepts and practices described within this document may be beneficial to other projects, so their application should be considered.

P.3 AUTHORITY

42 U.S.C. 2473 (c)(1), Section 203(c)(1) of the National Aeronautics and Space Act of 1958, as amended.

P.4 REFERENCES

a. NPD 1440.6, "NASA Records Management."

b. NPD 8700.1, "NASA Policy for Safety and Mission Success."

c. NPR 1441.1, "Records Retention Schedules."

d. NPR 2810.1, "Security of Information Technology."

e. NPR 5100.4, "NASA FAR Supplement."

f. NPR 7120.5, "NASA Program and Project Management Processes and Requirements."

g. NPR 8705.2, "Human Rating Requirements for Space Flight Systems."

h. NPR 8715.3, "NASA Safety Manual."

i. ANSI/ASQC Q9001-1994, "American National Standard: Quality Systems Model for Quality Assurance in Design, Development, Production, Installation and Servicing."

P.5 CANCELLATION

None.

/s/Michael A. Greenfield, Ph.D.
Acting Associate Administrator for Safety and Mission Assurance

CHAPTER 1. Risk Management Overview

1.1 Risk Management Concept

1.1.1 Risk.

Risk is characterized by the combination of the probability that a program or project will experience an undesired event (some examples include a cost overrun, schedule slippage, safety mishap, health problem, malicious activities, environmental impact, failure to achieve a needed scientific or technological breakthrough or mission success criteria) and the consequences, impact, or severity of the undesired event, were it to occur.

1.1.2 Risk Management.

Risk Management (RM) is a process wherein the program/project team is responsible for identifying, analyzing, planning, tracking, controlling, and communicating effectively the risks (and the steps being taken to handle them) both within the team and with management and stakeholders. As depicted in Figure 1, RM is a continuous, iterative process to manage risk in order to achieve mission success. It should be a key element and an integral part of normal program/project management and engineering processes.

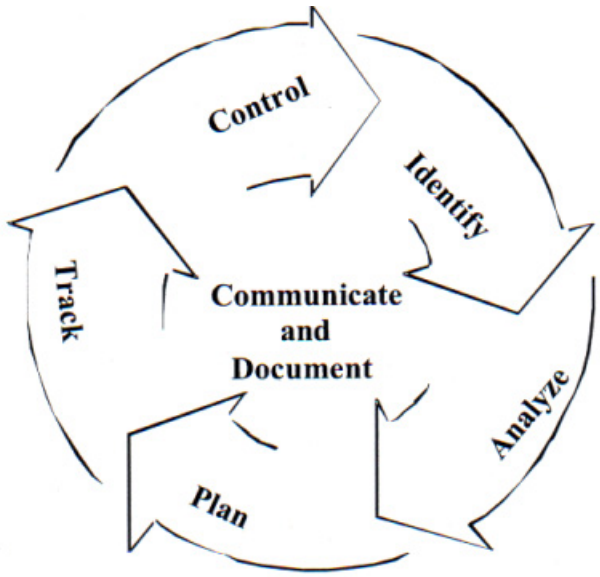

Figure 1. Continuous Risk Management (CRM)
Print

1.2 Risk Management Requirements

1.2.1 NPR 7120.5, "NASA Program and Project Management Processes and Requirements," provides the basic RM requirements that are applicable to all programs and projects under the scope of that NPR.

1.2.2 In addition to the RM requirements contained within NPR 7120.5, other RM and RM-related requirements are included within applicable regulations and other directives. Examples include NPR 5100.4, "NASA FAR Supplement," which includes requirements for RM within the context of acquisition planning, selecting sources, choosing contract type, structuring award fee incentives, administering contracts, and conducting contractor surveillance. NPR 2810.1, "Security of Information Technology," includes requirements for the identification and assessment of threats and vulnerabilities in order to pinpoint those areas that are most likely to be at risk should someone exploit a system or network vulnerability with the sole purpose of doing harm. NPR 8705.2, "Human Rating Requirements for Space Flight Systems," includes requirements related to risks associated with humans involved in or exposed to space flight activities. NPR 8715.3, "NASA Safety Manual," includes requirements related to safety risks. As appropriate, requirements from other sources such as these are referenced within this NPR.

1.2.3 Reserved.

1.3 Risk Management Responsibilities

1.3.1 The Program Manager (PM) is responsible for the following:

a. Applying a continuous risk management process within the program throughout its life cycle (Requirement 26006).

b. Documenting and approving that process within a Risk Management Plan (Requirement 30898).

c. Documenting and managing risks throughout the program's life cycle (Requirement 30899).

d. Approving the formal acceptance of all program risks (Requirement 30900).

e. Providing program risk status, especially concerning primary risks (see Appendix A, Glossary), to the Program Management Council (PMC) or Governing PMC as appropriate (Requirement 30901).

1.3.2 The Project Manager is responsible for the following:

a. Applying a continuous risk management process within the project throughout its life cycle (Requirement 26007).

b. Documenting and approving that process within a Risk Management Plan (Requirement 30902).

c. Documenting and managing risks throughout the project's life cycle (Requirement 30903).

d. Approving the formal acceptance/closure of all project risks (Requirement 30904).

e. Providing project risk status, especially concerning primary risks, to the Program Manager, Center Director, PMC, or Governing PMC as appropriate (Requirement 30905).

1.3.3 The PMC or Governing PMC is responsible for the following:

a. Evaluating the program/project's risk status and ensuring that the formal acceptance/closure of program/project risks is consistent with NASA's goals and requirements (Requirement 26008).

b. Concurrence on the acceptance of all primary risks (Requirement 30906).

1.3.4 The Safety and Mission Assurance (SMA) organizations at the NASA Centers are responsible for providing ongoing risk management consultation, facilitation, and training to program/project organizations (Requirement 26009).

1.3.5 The Systems Management Offices (SMO) at Centers and the Independent Program Assessment Office (IPAO) are responsible for assessing risk management as an element of their Independent Assessments (IA), Independent Annual Reviews (IAR), Non-Advocate Reviews (NAR), other independent reviews, or in their participation within regular program/project reviews (Requirement 26010). Appendix C provides a checklist for use in such assessments.

1.3.6 Headquarters Functional Offices (see Appendix A, Glossary) are responsible for the following:

a. Providing guidance concerning the identification, analysis, and mitigation of risks within their respective functional areas including support to their equivalents at the NASA Centers (Requirement 26011).

b. Supporting the PMC in the evaluation and assessment of programs/projects with respect to their risk management status within their respective functional areas (Requirement 30907).

1.3.7 Center Functional Offices are responsible for the following:

a. Providing support to programs/projects to assist in their identification, analysis, and mitigation of risks within their respective functional areas (Requirement 26012).

b. Supporting the Governing PMC in their evaluation and assessment of programs/projects with respect to their risk management status within their respective functional areas (Requirement 30908).

CHAPTER 2. Implementing the Risk Management Process

2.1 Overview of the Risk Management Process

2.1.1 RM begins early in program/project formulation and must continue in a disciplined manner throughout all program/project life cycle phases. A long-range view of the program/project and its mission success criteria, and open communication among all members of the program/project team (including stakeholders), are essential elements for successful RM.

2.1.2 Although different organizations refer to RM elements by different names, RM processes used for years by various organizations contain virtually the same essential core ingredients. For example, the IT security process as described in NPR 2810.1 considers threats (equivalent to undesirable events as used in the definition of risk in this NPR and NPR 7120.5), vulnerability (equivalent to likelihood (see Appendix A, Glossary) of occurrence as defined in this NPR) and impact (equivalent to consequences as defined in this NPR) as the key elements in identifying risk. The RM process identified in Figure 1 contains the basic elements of the process. Users may substitute other nomenclature as long as the requirements of all elements are satisfied. Details on each step of the process are provided in the following paragraphs.

2.2 Risk Identification

2.2.1 Risk Identification Concept.

The first step in the RM process is to identify the risks (technical and programmatic) specific to a program/project. As identified in NPR 7120.5, this entails identifying individual risks and clearly describing those risks in terms of both the undesirable event the risk presents as well as the consequences of that event to the program/project. In addition, risk identification includes identification of all the necessary information to place the risk in the context of the program/project. This is necessary to ensure that the original characterization of the risk can be understood by other personnel, particularly after time has passed. Risk identification shall be continued throughout the life cycle of the program/project.(Requirement 26015). In identifying risks, PM's should challenge even those things that have long worked successfully, and ask at least the following questions:

- "What can go wrong?"

- "What would be the consequences (to safety, mission objectives, schedule, cost) if it does go wrong?"

2.2.2 Risk Identification Inputs.

There are many useful sources of information that provide the input for risk identification, including the following:

a. Team members.

b. Previous analyses, lessons learned, and historical data. NOTE: Lessons learned from past projects are available from the NASA Lessons Learned Information System (LLIS) at: http://llis.nasa.gov/.

c. System safety and reliability analyses; e.g., hazard analysis, fault tree analysis, failure modes and effects analysis.

d. Expert interviews and external review boards (the NASA LLIS also provides access to selected Mishap Investigation Board Reports).

e. Data extrapolation based on review and analysis of compiled risk data.

f. Simulations, test data, and models.

g. Analysis of the work breakdown structure.

h. Comparison of mission objectives/success criteria, goals, assumptions, plans, and margins (maintained to address the "unknown unknowns").

i. Analysis of resources/schedule-review and analysis of required or available resources; continued monitoring of schedule milestones, and risk mitigation/planned action milestones.

j. Analysis of suppliers-review and analysis of the procedures and customer requirements of suppliers.

k. Analysis of proposed changes.

l. Test results.

m. Nonconformance reports.

n. Analysis of external factors that affect program/project risk; e.g., computer security assessments, physical security assessments, human factors performance assessments, environmental assessments.

o. Results of risk analyses from other programs, projects, and institutional areas that support or are critical to this program/project's success (for example, if a project requires the use of a test stand to perform critical tests and the test stand is currently undergoing refurbishment, the risks of completion of that refurbishment by the time needed for this project should be considered).

p. Risk understanding resulting from previous program(s) (heritage).

q. Tools and references as identified in Appendix D.

2.2.3 Risk Identification Outputs.

The primary output of risk identification is a statement of risk for each individual risk (see paragraph 2.7.5). These statements of risk are summarized in a comprehensive listing of program/project risks, or Risk List (see paragraph 2.7.6), which shall be established and maintained to reflect the current understanding of risks within the program/project (Requirement 26017).

2.3 Risk Analysis (Evaluation, Assessment, or Estimation)

2.3.1 Risk Analysis Concept.

In analyzing risks, PM's should ask at least the following questions:

How likely is it for this risk to occur?

How soon do we need to act on this risk?

How does this risk compare with other risks?

As identified in NPR 7120.5, risk analysis consists of estimating the likelihood and the consequences of the risk and the timeframe in which action must be taken on an identified risk to avoid harm. Estimates may be quantitative or qualitative, but should be stated and combined in such a way that identified risks can be prioritized (compared to each other or to relevant criteria and ranked from highest to lowest) in terms of mission impact. Methods of analyzing risk include, but are not limited to, the following:

a. Individual or group expert judgment.

b. Statistical analysis of historical data.

c. Uncertainty analysis of cost, performance, and schedule projections (consists of building and running a probabilistic model of the system under investigation, including the chance variation inherent in real-life cost, performance, and schedule).

d. Probabilistic Risk Assessment (PRA) (see Appendix A, Glossary) (also known as Probabilistic Safety Assessment (PSA) and Quantitative Risk Assessment (QRA)).

e. Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA).

f. Ordinal risk scales.

g. Comparison to analogous systems.

Before prioritizing, the risks should be classified or grouped with similar risks. There are several purposes for classification. One purpose of classification of risks is to understand the nature of the risks and to group related risks so as to build more cost-effective mitigation plans. Another purpose is to identify risks that are equivalent or duplicate each other and combine them as appropriate. Additionally, risks are classified so that they can be tracked and monitored by various elements of the program. For example, a functional area such as financial or safety may want to concentrate on the subset of risks within their functional area to assure that all these risks are adequately resolved. Perhaps all the risks related to the acquisition process maybe classified together for purposes of performing acquisition planning or source selection. Once classified, the risks should be prioritized. The purpose of prioritization is to sort through a large number of risks and determine which are the most important and, therefore, should be dealt with first.

One widely used qualitative method of prioritizing risks is through the use of a Risk Assessment Code (RAC). Other methods of prioritization include multivoting (quantitative) and attribute assignment (qualitative). The RAC method combines qualitative and semi-quantitative measures of risk likelihood with similar measures of risk consequences to yield a RAC that can be the basis for initial prioritization of risks. For example, a risk having a consequence of "Class II - Critical" and a likelihood of "A - Likely to occur," would have a RAC of 1, and would be a top priority for mitigation. The following paragraphs provide guidance in using the RAC. In addition, the RAC methodology can be tailored to fit the needs, complexity, or experience base of a program/project.

2.3.1.1 Consequence.

Consequence is an assessment of the worst credible potential result(s) of a risk. The measurement units differ depending on the

specific risk. For example, the consequence of a cost risk may correspond to specific dollar amounts or percentages of the program/project budget or the consequence of schedule risks may correspond to the length of time delays. Consequence classifications are defined generally as Catastrophic, Critical, Marginal, and Negligible. A sample classification approach might be as follows:

a. Class I - Catastrophic. A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission; schedule slippage causing launch window to be missed; cost overrun greater than 50 percent of planned cost.

b. Class II - Critical. A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware; schedule slippage causing launch date to be missed; cost overrun between 15 percent and not exceeding 50 percent of planned cost).

c. Class III - Moderate. A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware; internal schedule slip that does not impact launch date; cost overrun between 2 percent and not exceeding 15 percent of planned cost.

d. Class IV - Negligible. A condition that could cause the need for minor first aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware more than normal wear and tear level; internal schedule slip that does not impact internal development milestones; cost overrun less than 2 percent of planned cost.

Note: The portions of these classifications concerning safety are defined within NPR 8715.3, "NASA Safety Manual."

2.3.1.2 Likelihood.

Likelihood is the probability that an identified risk event will occur. The following is as example of likelihood categories:

a. Likelihood A. Likely to occur (e.g., probability > 0.1).

b. Likelihood B. Probably will occur (e.g., 0.1 $\geq$ probability > 0.01).

c. Likelihood C. May occur (e.g., 0.01 $\geq$ probability > 0.001).

d. Likelihood D. Unlikely to occur (e.g., 0.001 $\geq$ probability > 0.000001).

e. Likelihood E. Improbable (e.g., 0.000001 $\geq$ probability).

2.3.1.3 Risk Matrix.

The risk matrix in Figure 2 shows the application of consequence and likelihood in determining a RAC and a qualitative (high, medium, low) risk rating.

	LIKELIHOOD ESTIMATE				
CONSEQUENCE CLASS	**A**	**B**	**C**	**D**	**E**
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

High Risk	
Medium Risk	

Figure 2. Risk Matrix Showing Risk Assessment Codes (RAC)

2.3.1.4 Timeframe.

Timeframe is the time in which action must be taken to handle the analyzed risk or the time period in which the program/project will be impacted by it. Timeframe may be used to order RAC's. For example, a RAC 1 risk with a "near-term" timeframe should be worked before a RAC 1 risk with a midterm or far-term timeframe. The following is an example of timeframe categories for a three year long program:

a. Near-term. The project must take action on the identified risk or will be impacted by the risk in the next 90 days.

b. Midterm. The project must take action on the identified risk or will be impacted by the risk in the next 90-180 days.

c. Far-term. The project need not take action or will not be impacted by the risk in the next 180 days.

2.3.2 Risk Analysis Inputs.

There are many useful sources of information that provide the input for risk analysis including the following:

a. Risk data generated in other steps in the process.

b. Test data.

c. Expert opinions.

d. Hazard Analyses, Failure Modes and Effects Analyses.

e. Lessons learned data and historical information from other programs/projects.

f. Probabilistic Risk Assessments (PRA).

g. Technical analyses resulting from other activities, for example electromagnetic compatibility/interference analyses, software verification and validation activities.

2.3.3 Risk Analysis Outputs.

The primary outputs of risk analysis are clear estimations of the consequences of the risk, the likelihood of the risk's occurrence, and the timeframe in which an action must be taken on an identified risk. This information is included and documented in the Risk List (see paragraph 2.7.6). Information obtained within the classification portion of the process eliminates duplicate risks from the Risk List and links risks where there may be an advantage in addressing these risks together for purposes of risk planning. Finally, based upon the primary outputs of the risk analysis, the risks are prioritized with the prioritization documented in the Risk List.

2.4 Risk Planning (Handling, Treatment, or Decisionmaking)

2.4.1 Risk Planning Concept.

Once the risks have been identified and analyzed, the next step is to plan the action that should be taken on each risk. In this case, the PM should at least ask the following questions:

"What can we do to prevent it from going wrong, or at least reduce the probability or severity of the consequences?"

"Who should be assigned to take these preventive actions?"

As described in NPR 7120.5, risk planning consists of assigning responsibility to determine the approach to respond to the identified risks and, if a decision is made to mitigate the risk, the subsequent development and implementation of the action to mitigate the risk. As each identified risk is assigned to a member of the program/project team or matrixed professional from another organization, it is that person's responsibility to determine the approach to respond to each assigned risk. The approaches for responding to risk are as follows:

a. Mitigate. Risk mitigation may be achieved by applying methods aimed at eliminating the risk or reducing the likelihood and/or consequence of a risk. This may be accomplished through engineering, schedule, or budgetary changes to designs, processes, or procedures; or alternate paths and approaches.

b. Accept. The PM shall establish the criteria for accepting risks, document the rationale for accepting individual risks and include the signed formal acceptance within the risk acceptance records. (Requirement 26025). One criteria for accepting risk is to have a documented, tested, and signed contingency or recovery plan in place to respond to the consequences of an accepted risk should that risk manifest itself as an undesired event.

c. Research. This includes the collection of additional information, evaluation, and reporting of results on which to base future decisions or, sometimes, to reduce the uncertainty surrounding risk estimates.

d. Monitor. This includes deciding not to take immediate action, but to track, survey, or watch the trends and behavior of risk indicators over time. If the mitigate approach is selected, the person assigned to the risk is responsible for determining the level of the scope of the mitigation, establishing the goal(s) of the mitigation effort and determining the resources required to implement the mitigation. (The scope of the mitigation includes the development of either an action item or a detailed task plan, both of which are referred to as risk mitigation plans). In addition, the person assigned to the risk is responsible for coordinating mitigation activities with the person who initially identified the risk, appropriate functional offices, and other persons assigned responsibilities for risks to ensure that the mitigation activities address all concerns and do not increase or introduce additional risk in another area.

2.4.2 Risk Planning Inputs.

The basic inputs to Risk Planning are the outputs from Risk Identification and Risk Analysis elements of the overall risk management process. The primary new input is the resources available within the program to be applied to mitigation action items or task plans. Development and implementation of the risk mitigation plans or, in the case of a risk acceptance decision, contingency or recovery plans, may be constrained by the resources available. Program/projects will want to carefully determine which mitigations provide the most improvement in risk. Analytical tools, such as cost-benefit analysis and PRA, can assist in helping to determine how to allocate limited resources among the mitigation actions that can provide the optimal improvement to the program/project's risk posture.

2.4.3 Risk Planning Outputs.

The outputs of risk planning are as follows:

a. Updates to the Risk List (see paragraph 2.7.6) to identify the assignment of a person to respond to the risk, and the identification of what action is to be taken with respect to the risk.

b. Individual risk mitigation plans (see paragraph 2.7.7), linked to the risk list, for each risk involving a decision to mitigate.

c. In the case of a decision to accept the risk, the acceptance rationale as included in the risk acceptance records (see paragraph 2.7.8).

2.5 Risk Tracking (Monitoring or Verification)

2.5.1 Risk Tracking Concept.

Risk tracking is used to measure the progress of the risk management program. In this area the PM should ask at least the following questions:

- "Are risk mitigation actions effectively mitigating risk and are the actions within budget and schedule constraints?"

- "Is the overall risk for the program/project increasing or decreasing?"

- "If the overall risk for the program/project is decreasing is it decreasing to the maximum practicable extent?

Risk tracking involves collecting, updating, compiling, organizing and analyzing risk data and reporting risk trends to determine whether particular risks are decreasing, staying the same, or increasing over time. Tracking focuses primarily on risks identified for mitigation, research, and monitoring, although all risks, including accepted risks, should also be tracked to ensure that conditions or assumptions have not changed to the point that reevaluation is necessary. For research actions, tracking serves to assure that the research efforts are progressing satisfactorily and that the identified timeframe still permits further research. Risk tracking should provide the insight on which to draw conclusions about the effectiveness of mitigation actions, or the need to take action on monitored risks that are increasing toward or beyond a trigger level. "Trigger" levels are the warning or control limits often used in statistical process control. Trigger levels (see Appendix A, Glossary) may be predetermined for particular risks (if the risks are being monitored) to signal the need for action. Trigger levels also identify those effects on the overall program/project, not only relative to the critical path but also to the resources and performance results; critical decisionmaking points; variations on systems capabilities; and other elements. Tracking results should be made readily available to the program/project team members. The frequency for checking tracking results and trigger levels should be such that the program/project team will have adequate time to react to adverse trends.

2.5.2 Risk Tracking Inputs.

Tracking of a particular risk requires knowledge of its data elements (including any metric(s)) from the Risk List, the applicable mitigation plan or tracking requirements (for watched risks), resources available for mitigation, and possibly other relevant program/project data (such as cost and schedule variances, critical path changes, and program/project performance indicators).

2.5.3 Risk Tracking Outputs.

The outputs of risk tracking are primarily risk status reports on the current program/project risk posture (see Appendix A, Glossary).

2.6 Risk Control (Feedback)

2.6.1 Risk Control Concept.

Risk control is the feedback process of reevaluating, based on recent tracking information, what actions to take concerning a particular risk, and implementing those decisions. The PM should be asking at least the questions:

"What risks still need to be researched?"

"What risk mitigations need to be revised?"

"Have risks reached a point (trigger level) where a contingency plan needs to be invoked?"

"What risks can be accepted and formally closed?"

Actions may include changing the current action plan, closing the risk (accepting the residual risk), invoking a contingency plan when the original plan is found to be ineffective, or continuing with the original plan and continuing to track the risk. Each of the risks identified, analyzed, planned, and tracked should be periodically reviewed (preferably monthly) to ensure that decisions made are effective and that associated actions remain applicable. Since NPR 7120.5 requires that **all** risks be dispositioned before delivery to operations, or the equivalent for a technology program, the program/project shall review and ensure that **all** risks are dispositioned before this milestone (Requirement 20631).

2.6.2 Risk Control Inputs.

All of the information developed as a part of the risk management process to this point, including the risk list and the risk mitigation plans, form the inputs to risk control.

2.6.3 Risk Control Outputs.

The outputs from risk control are decisions made by the PM, or appropriate decisionmaker, with respect to risk. The decisions reflect the program/project's authorization to apply one of the approaches for responding to risk identified within the risk planning element of the risk management process. Decisions, or revalidation of those decisions, to mitigate, research, or monitor risk would be documented in accordance with program practices and would be reflected within the Risk List. The decision to close an identified risk shall be formally documented with signatures of the PM, the person having assigned responsibility for the risk, and the person that identified the risk (Requirement 26033). In addition, the GPMC must concur with the acceptance of all primary risks (Requirement 30909).

2.7 Documenting and Communicating Risk

2.7.1 General.

Effective RM requires open, clear, and ongoing communication within the program/project team. The RM documentation process ensures that RM policies are established, understood, implemented, and maintained, and that a formal audit trail is developed to establish the origin of, and rationale for, all risk-related decisions. RM documentation shall be readily accessible to the entire team; e.g., in an automated form, and under configuration control. , (Requirement 26034). The RM process draws on existing project documentation to the maximum extent possible. RM documentation and records are maintained in accordance with the requirements of NPD 1440.6, "NASA Records Management," and NPR 1441.1, "Records Retention Schedules," and as documented in the Risk Management Plan. In addition to the requirements of NPD 1440.6 and NPR 1441.1, documentation of the inputs, analyses, and outputs of each element of the RM process may also be considered by the Center to be quality records as defined by ANSI/ASQC Q9001-1994.

2.7.2 Program/Project Plan.

The Program/Project Plan, as required by NPR 7120.5, includes a summary of the basic risk management planning for the program/project. The implementation of the basic strategy/philosophy for program/project risk management described in the Program/Project Plan is then further detailed within the Risk Management Plan. The Program/Project Plan is also the location where the acceptable risk (see Appendix A, Glossary) level for the program/project is defined and documented and a summary of the primary risks for the program/project is documented.

2.7.3 Acquisition Plan.

The Acquisition Plan, developed in conjunction with the Acquisition Strategy Meeting, is required by the NASA FAR Supplement (NFS) 1807.105. The requirements for the Acquisition Plan include many risk management items. Specifically, the Acquisition Plan is required to do three things related to risk management. First, it discusses the Program's/Project's risks (including a quantification (magnitude of risk). Second, it discusses how to structure the acquisition approach to manage risks, and third, it identifies decisions made to accept, mitigate, track and/or research acquisition risks. The Risk List (paragraph 2.7.6), Risk Acceptance Records (paragraph 2.7.8), and Risk Mitigation Plans (paragraph 2.7.7) provide the core data to develop the risk management portions of the Acquisition Plan and support completion of the Acquisition Strategy Meeting.

2.7.4 Risk Management Plan.

2.7.4.1 Risk Management Plan General.

As specified in NPR 7120.5, "NASA Program and Project Management Processes and Requirements," every program/project shall have an RM Plan (Requirement 26037). This stand-alone plan, approved by the PM during the Formulation Subprocess, should be an integral element of the program/project documentation. The RM Plan shall be placed under formal configuration control (Requirement 30910). The RM Plan should be reviewed and updated as necessary when a change in program phase occurs, or when significant changes in success criteria, program architecture, or design occur. The RM Plan shall be available for review by the GPMC (Requirement 30911). Note: In developing the Risk Management Plan, keep in mind that other requirements and guidance such as those documented in the NFS, NPR 2810.1, "Security of Information Technology," and NPR 8715.3, "NASA Safety Manual," will need to be considered and addressed accordingly.

2.7.4.2 Risk Management Plan Content.

2.7.4.2.1 The RM Plan shall be program/project specific, configuration controlled, and include the following (incorporating technical information by reference) (Requirement 26038):

a. Introduction. Explain the purpose, scope, assumptions, success criteria, constraints, processes, and key ground rules pertaining to the program/project RM process.

b. Overview of Risk Management Process. Provide an overview of the RM process and information flow; describe how the RM process integrates and relates to other program/project management activities. Include general risk mitigation strategies to be employed throughout program/project implementation.

c. Organization. Provide an explanation of the organization, roles, and responsibilities of the program/project with respect to risk management. Provide a clear indication of where and how customers and suppliers interact with the organization, including specific responsibilities if appropriate. Consider the use of a Responsibility Assignment Matrix to help document the responsibilities. Provide an explanation of how team members will be trained in the application of RM methodology.

d. Process Details. Provide the RM process details and related procedures, methods, tools, and metrics. Identify the process and considerations to be used in determining the level of indenture to which the risk analyses are to be conducted. Include in this section, or in an appendix, the specific methodologies to be used for risk identification, analysis, planning, tracking, and controlling. Include the process to be used for prioritization of risk, identification of risk acceptance criteria, application of resources to risks, and continual assessment of the program/project risk profile. Describe how risk information will be communicated both internally to the program/project staff and throughout the management chain. Document links to other risk-related requirements, processes, and products, such as processes and products defined within related IT Security Plans as required by NPR 2810.1 and Acquisition Plans required by the NASA FAR Supplement.

e. Resources and Schedule of Risk Management Milestones. Show schedule, milestones, and allocation of resources for RM activities, including resource reserves (contingency) that might be available for risk mitigation.

f. Documentation of Risk Information. Specify the format and data elements that will comprise the program/project Risk List (see paragraph 2.7.6 for a suggested format). Document where and how the list will be maintained, how configuration control will be applied, how the list will be used, and how often it will be updated/reviewed. Tell how team members will be able to access the current list at any time. When applicable, address intra- as well as inter-programmatic considerations; e.g., spacecraft-to-spacecraft and spacecraft-to-environmental systems dependencies, resources outside the program/project's control such as wind tunnel access, test facilities, launch facilities, support aircraft, IT resources that are vital to the success of the program, which might affect risk. (Recommend that the format be set, with a minimal number of elements, to allow database compilation). Specify the format, content, and schedule of all other RM documentation used within the program/project, such as Risk Mitigation Plans and Risk Acceptance Records.

g. Methodology Associated with Program/Project Descope. Discuss the program/project descope (see Appendix A, Glossary) methodology that might be applied when risk mitigation cannot be accomplished due to limited resources (cost, schedule, workforce). Note: Limited resources are not an excuse for not meeting legislated or otherwise mandated requirements. This discussion should include identification of organizations that would be impacted by the identified descoping (for example, if the descoping involved changes to contracts, the appropriate procurement organizations would need to be involved). Describe the point in the descoping process at which the program/project would no longer meet sufficient mission objectives or success criteria to be considered viable.

2.7.4.2.2 The CRM website, http://crm.nasa.gov/ and the Process Based Mission Assurance Knowledge Management System, http://pbma.hq.nasa.gov/ contain sample RM plans, a template for preparing them, and additional templates for tailoring RM to a specific project, whether large or small.

2.7.5 Statement of Risk.

The Statement of Risk is a clear, concise, and complete statement of the risk. In general, risk statements are written in a condition - consequence format (that is "given the there is a possibility that will occur"). It can be supported by additional information if required to place the risk in context or explain the assumptions associated with the risk. If supporting information is required the Statement of Risk should be clearly linked to that information and where it is maintained.

2.7.6 Risk List.

2.7.6.1 Every program/project shall have a Risk List. (Requirement 26065). The Risk List is the listing of all identified risks in

priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the project. Risk prioritization is performed by the project team and consolidated and approved by the PM. Figure 3 provides suggested data elements and format for the Risk List.

Priority	Risk Statement	Risk Tracking Identifier	Risk Originator	Consequence	Likelihood	Timeframe	RAC	Classification	Primary Risk	Responsible Person
1										
2										
3										
4										

Figure 3. Risk List

KEY:

Priority - Enter the priority for the identified risk.

Risk Statement - Enter a clear, concise statement of the risk. If additional information is required to place the risk in context or explain the assumptions associated with the risk, identify where that information is maintained.

Risk Tracking Identifier - Provide a unique identifier for the risk for tracking purposes.

Risk Originator - Identify the person who identified the risk and can provide background information concerning the risk.

Consequence - Identify the consequence of the risk (including, but not limited to cost, performance, schedule impact, and personnel illness/injury).

Likelihood - Identify the likelihood of the risk occurring.

Timeframe - Identify the timeframe when action on the risk needs to be completed.

RAC - Enter the appropriate RAC for the identified risk.

Classification - Identify any subdivisions or groupings of risks.

Primary Risk - Indicate if the risk is a primary risk (yes/no).

Responsible Person - Identify the person assigned to provide the risk response.

Risk Response - Identify what response has been designated for the risk (Mitigate, Accept, Research, Monitor). If a risk has been accepted, identify where the risk acceptance is documented. If a risk is mitigated, identify the appropriate risk mitigation plan.

Metrics - Identify any metrics related to the risk that are being used for tracking/trending.

2.7.6.2 The Risk List must be updated as changes (including changes in assumptions) occur (Requirement 26063). Extracts from the list shall be presented at project meetings, reviews, and milestones as required by the RM Plan (Requirement 30912). Programs/projects may also find it beneficial to use the classification of risks to create subsets of the Risk List in addition to the complete Risk List so that working or functional groups may focus on specific areas of risk (for example, tracking all of the environmental risks or the security risks or technical risks together). The Risk List must be widely accessible to all members of the program/project team (Requirement 30913).

2.7.7 Risk Mitigation Plans.

These plans describe actions to mitigate identified risks, as well as risk measures, indicators, and trigger levels used in the tracking of the risks and the effectiveness of their mitigation actions. These plans also include the cost and schedule information required to implement the plan. The program/project determines the format for the plans (which could range from simple action items for relatively simple mitigations to formal task plans for more complex mitigations) consistent with other program/project planning documentation.

2.7.8 Risk Acceptance Records.

These records document program/project acceptance of risk (and, if a primary risk, GPMC concurrence). The program/project determines the format of these records consistent with other program/project documentation (for example, program/project configuration management processes and documentation could be used to document acceptance of risk). The risk acceptance records include the risk acceptance rationale, as well as the appropriate signatures for approval, including revalidations as required.

2.7.9 Risk Trends.

These consist of displays (graphical, tabular, or textual) showing changes to risk indicators over time; i.e., decreasing, staying the same, or increasing. Trends should be updated frequently, on a schedule documented in the RM Plan, so that the program/project team will have adequate time to react to adverse trends. Risk trend documentation should also be consistent with other program/project metrics information.

2.7.10 Risk Profile.

Beginning early in a project, the PM should make a qualitative or quantitative projection of overall expected risk trend (technical risks, as well as programmatic risks) over the life of the program/project (showing major milestones). A risk profile such as the example shown in Figure 4 should be constructed. Initially, the projected risk profile (that part that lies in the future) should be annotated to explain significant, but expected, changes in risk. Over the life of a program/project, the risk profile should be updated regularly, as documented in the RM Plan, to reflect actual changes in risk. Explanations for these changes should be annotated on the profile for briefing at major milestone meetings.

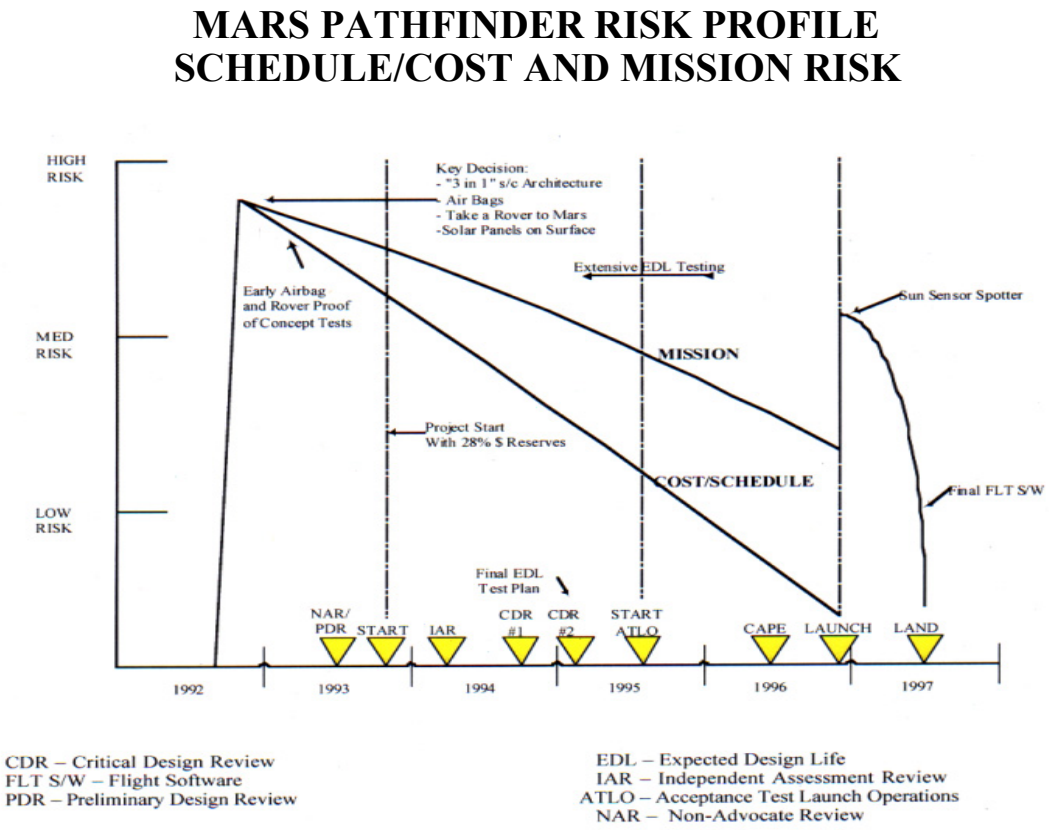

Figure 1. Continuous Risk Management (CRM)
Print

Figure 4. Risk Profile Example (Mars Pathfinder, constructed post-mission)

Note: The terms Technical and Programmatic Risk used in this NPR are roughly equivalent to the terms Mission Risk and Cost/Schedule Risk, respectively as they are used in this figure.

2.7.11 Risk Communication.

2.7.11.1 Early in a program/project, the PM should develop a risk communication strategy. It should address how risk will be openly and clearly communicated within the program/project team, with management, stakeholders, appropriate functional offices, other government entities, and the public, throughout the life cycle of the program/project.

2.7.11.2 Consideration should be given to establishing a program/project RM database to provide an easily accessible way to store program/project risk information and thereby aid every step of the RM process. This would also provide a risk record archive, making tracking and analyzing risk, past methods, and results available for all to view.

APPENDIX A. Glossary

Acceptable Risk. The risk that is understood and agreed to by the program/project, GPMC, Enterprise, and customer, and sufficient to achieve the defined success criteria within the approved level of resources (source - NPR 7120.5).

Descope. Reduction or elimination of elements of a program/project that can be accomplished while still permitting the program/project to meet the critical program/project objectives. If the program/project has been descoped to a point where the critical program/project objectives cannot be met, then a termination review may be required.

Functional Offices. Headquarters Functional Offices include the Offices of the Chief Financial Officer, Chief Engineer, Chief Information Officer and Chief Scientist as well as Equal Opportunity Programs, Human Resources, General Counsel, Procurement, External Relations, Institutional and Corporate Management, Small and Disadvantaged Business Utilization, Legislative Affairs, Public Affairs, Safety and Mission Assurance, Security Management and Safeguards and Office of Health and Medical Systems.

Life Cycle. The entire course of a program/project from inception in the formulation subprocess to completion in the implementation subprocess.

Likelihood. The probability that an identified risk event will occur.

Primary Risk. Those undesirable events having both high probability and high impact/severity (source - NPR 7120.5).

Probabilistic Risk Assessment. A systematic, logical, and comprehensive tool to assess risk (likelihood of unwanted consequences) for the purpose of 1) characterizing and improving system performance and mission success, 2) increasing safety in design, operation and upgrade, and 3) saving money in design, manufacturing or assembly, and operation.

Program. A major activity within an Enterprise having defined goals, objectives, requirements, and funding levels, and consisting of one or more projects (source - NPR 7120.5).

Project. An activity, designated by a program, characterized as having defined goals, objectives, requirements, a Life Cycle Cost (LCC), a beginning, and an end (source - NPR 7120.5).

Risk. The combination of 1) the probability (qualitative or quantitative) that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough; and 2) the consequences, impact, or severity of the undesired event were it to occur (source - NPR 7120.5).

Risk Management. An organized, systematic decisionmaking process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving program/project goals (source - NPR 7120.5).

Risk Posture. The program/project's level of risk.

Trigger Levels. Warning or control limits applied to the level of risk.

APPENDIX B. Acronyms

ASQC	American Society for Quality Control
ANSI	American National Standards Institute
CRM	Continuous Risk Management
DoD	Department of Defense
FAR	Federal Acquisition Regulations
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GPMC	Governing Program Management Council
IA	Independent Assessment
IAR	Independent Annual Review
IPAO	Independent Program Assessment Office
JPL	Jet Propulsion Laboratory
LLIS	Lessons Learned Information System
NAR	Non-Advocate Review
NASA	National Aeronautics and Space Administration
NFS	NASA FAR Supplement
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
PM	Program/Project Manager
PMC	Program Management Council
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
QRA	Quantitative Risk Assessment
RAC	Risk Assessment Code
R-BAM	Risk-Based Acquisition Management
RM	Risk Management
SMA	Safety and Mission Assurance
SMO	Systems Management Office
SOLAR	Site for On-line Learning and Resources
U.S.C.	United States Code

APPENDIX C. Checklist for Assessment of Risk Management

This checklist is intended for the use of the NASA Independent Program Assessment Office (IPAO) at Langley Research Center, or Center Systems Management Offices (SMO), when assessing the RM activities conducted by program/project offices.

Risk Management Process

Does the program/project use a Continuous Risk Management process?

Was the Risk Management process originated during formulation?

Does the Risk Management process adequately address all risk management requirements as documented in the NASA FAR Supplement and NASA Directives (for example, NPR 7120.5, NPR 8000.4, NPR 2810.1, NPR 8715.3, etc.)?

Is RM a part of the normal business of program/project meetings? This is preferred as opposed to RM conducted in special, splinter meetings. Copies of program/project meeting minutes showing RM activities being conducted should be requested.

Are adequate resources applied to the Risk Management effort?

Risk Identification

How are risks identified?

Is the identification process effective?

Risk Analysis

How are risks analyzed? For example, does the project employ Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), or Probabilistic Risk Assessment (PRA)?

Is the analysis process effective?

Has each risk been assessed and quantified as to probability and consequences (including cost consequences)?

Are risks prioritized?

Are risks updated when a change in program phase occurs, or when significant changes in program scope, budget, or schedule occur?

Risk Planning

Has responsibility to address each risk been assigned to a person?

Have mitigation plans been prepared/implemented?

Have adequate resources been assigned for effective implementation of the risk mitigation plans?

Risk Tracking

How are risks and risk trends tracked?

Is the risk tracking effective?

Are all mitigated and monitored risks being regularly tracked to ascertain trends and ensure that trigger levels are not being exceeded?

Does the program/project maintain a risk profile such as that illustrated in paragraph 2.7.10 of this document? A copy should be

requested.

Risk Control

Was the acceptance of primary risks accomplished early and with the concurrence of the GPMC? Are these considered open or closed?

Were all risks dispositioned prior to delivery?

Risk Documentation

Does the program/project have an RM Plan document signed by program/project management? A copy of the RM Plan should be requested.

Do the contents meet the intent of the requirements of paragraph 2.7.4 of NPR 8000.4?

Does the program/project have a Risk List? A copy should be requested of at least a sample of the list.

Is the Risk List easily accessible to program/project team members?

Are all risk acceptances documented in accordance with the requirements of NPR 8000.4?

Risk Communication

Are risks regularly presented by the program/project to the GPMC? Copies of representative presentations should be requested.

Is a system RM database used as a tool to provide current, up-to-date information to the program/project team and all involved parties?

APPENDIX D. Sources of Additional Risk Management Assistance/Information/Tools

1. Consultation/Facilitation

RM consultation/facilitation is available from NASA Center SMA, SMO, and CFO offices. Available services vary from Center to Center but may include:

a. Arranging or actually conducting the RM training for the program/project staff.

b. Reviewing, or assisting in preparation of, the final Program/Project RM Plan.

c. Facilitating initial program/project team sessions or facilitating all team sessions to identify, analyze, plan, track, control, and communicate and document program/project risks.

d. Providing access to data or providing actual data from SMA databases (e.g., problem/failure reports, hazard reports, lessons learned) to support any of the steps in the RM process.

e. Assisting in the establishment of, or actually establishing and maintaining, a program/project risk database.

f. Introducing methods/tools which can be used to accomplish any or all steps of the RM process or actually applying the tools to produce the outputs needed by the program/project.

2. Web-Based Education and Training

A number of RM-related education and training modules are available to people who have a NASA Internet address; i.e., xxx@nasa.gov. The training modules can be found at the NASA Site for On-line Learning and Resources (SOLAR) at:

https://solar.msfc.nasa.gov:443/solar/delivery/public/html/newindex.htm

3. Classroom-Based Training

NASA Continuous Risk Management (CRM) Course, taught by the Systems Management Office, NASA Goddard Space Flight Center. Additional information about this training course can be found at: http://crm.nasa.gov/.

NOTE: Most NASA Centers have instructors who have been certified to teach the above course. Check your NASA Center SMA office for onsite availability of this training.

4. Textbook

The NASA RM paradigm, found in this document and in all of the above training, is based on NASA's work with the Software Engineering Institute at Carnegie Mellon University, and is consistent with the material found in the following textbook:

Continuous Risk Management Guidebook, Software Engineering Institute at Carnegie Mellon University, 1996, NTIS#: AD-A319533KKG, DTIC#: AD-A319 533\6\XAB.

5. Additional RM Guidance

Additional RM and RM-related guidance can be found in:

a. The Department of Defense, "Risk Management Guide for DoD Acquisition," Defense Acquisition University and Defense Systems Management College, Second Edition, May 1999. This document can be downloaded free of charge at the time of this writing from: http://www.dsmc.dsm.mil/pubs/pubsgen.htm.

b. Information on risks associated with computer systems can be found in the National Institute of Standards and Technology (NIST) publication, "Special Publication 800 - 12 - An Introduction to Computer Security: The NIST Handbook," available at:

http://csrc.nist.gov/publications/nistpubs/800-12/.

c. Information on implementation of Risk-Based Acquisition Management (R-BAM) can be found at: http://www.grc.nasa.gov/WWW/spaceiso/rbam/.

6. RM Tools

a. The latest information on RM tools, techniques, and case studies as applied to selected NASA programs may be found at: http://www.hq.nasa.gov/office/codeq/risk/risk.htm

b. NASA Reference Publication 1358, "System Engineering Tool Box for Design-Oriented Engineers," available from the NASA Scientific and Technical Information Office's Technical Report Server at http://www.sti.nasa.gov/index.html, contains summary information on a large number of systems engineering tools and methods, many of which are useful to RM.

c. The NASA Lessons Learned Information System (LLIS) contains lessons learned from past programs as well as selected Mishap Investigation Board Reports. The LLIS is at http://llis.nasa.gov/

d. The Risk-Based Acquisition Management website at http://www.grc.nasa.gov/WWW/spaceiso/rbam/ includes a tool to analyze data during the acquisition process.